DATE(S) ISSUED:
11/10/2009

SUBJECT:
Vulnerability in Microsoft Office Word Could Allow Remote Code Execution (MS09-068)

OVERVIEW:
A vulnerability has been discovered in Microsoft Office Word. This vulnerability can be exploited by opening a specially crafted Word document. The document may be received as an email attachment, or by visiting a web site where the document is hosted. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

SYSTEMS AFFECTED:

    Microsoft Office XP
    Microsoft Office 2003
    Microsoft Office 2004 for Mac
    Microsoft Office 2008 for Mac
    Open XML File Format Converter for Mac
    Microsoft Office Word Viewer
    Microsoft Office Word Viewer 2003

RISK:

Government:
    Large and medium government entities: **High**
    Small government entities: **High**

Businesses:
    Large and medium business entities: **High**
    Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been identified in Microsoft Office Word that could allow remote code execution. This vulnerability can be triggered by opening a specially crafted Word document which may cause a buffer-overflow condition due to a malformed record value. This vulnerability can be exploited via an email attachment or through the Web. In the email based

scenario, the user would have to open the specially crafted Word document as an email attachment. In the Web based scenario, a user would have to be convinced to visit a website and then open the specially crafted Word document that is hosted on the page. When the user opens the Word document the attacker's supplied code runs.

Please note that Microsoft Office XP or higher will, by default, prompt the user to Open, Save, or Cancel when accessing Office files in a Web or e-mail based scenario.

Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to download or open files from un-trusted websites.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS09-068.mspx

Security Focus:
http://www.securityfocus.com/bid/36950

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3135